REMARKS

Applicants are gratcful to the Examin r for the thorough and thoughtful office action of June 7, 2002, and the telephone interview of August 16, 2002, and offer the below remarks and summary of the interview. Applicants also respectfully request entry of new claims 36-40, discussed further below.

Objection to Claim 16

Applicants respectfully traverse the objection to claim 16, which requires claim 16 to be amended to be dependent from claim 1, since the two claims relate to different subject matter, and therefore cannot be dependent from each other. In particular, claim 16 involves a method for authenticating a uscr transaction, whereas claim 1 involves a method of administering registration of personal information in a data base. Accordingly, applicants respectfully traverse the objection to claim 16, and request reconsideration and allowance of claim 16.

Distinctions of Claimed Subject Matter over Pare Jr. et al. '879 and Bianco et al. '737

An embodiment according to applicants' claim 1 involves a method of administering registration of personal information in a data base in a manner directed to assuring the integrity of the personal information. A key to assuring the personal information's integrity, in accordance with an embodiment of applicants' invention, is to require a comparison of a set of newly provided physiological identifiers (sometimes called "biometrics"), from a subject, with a stored set of physiological identifiers, at a time when an attempt is made to modify information in a stored data set. See, for example, element (d) of applicants' claim 1; similar elements are found in claims 17, 29, 30, and 31. The stored data set includes both the user's personal information (such as a social security number, bank account number, etc.) and the stored set of physiological identifiers. An embodiment according to applicants' claim 1 therefore involves requiring a biometric match as a condition for modification of personal information associated with an account.

By contrast, as described in the office action, Pare Jr. et al. does not disclose or suggest requiring a biometric match for modification of personal information. Pare Jr. et al. uses a biometric comparison for access to a financial account through an ATM (automated teller machine), but not for providing added security for modification of the personal information associated with the account, including potentially even the account number itself. Whereas Pare Jr. et al. concerns gating access to funds, an embodiment according to applicants' claim 1 relates to gating modification of personal information associated with the account.

In terms of the language of applicants' claim 1, Pare Jr. et al. therefore does not disclose or suggest element (d): permitting a subject to modify information in a stored data set pertinent to a user only if (i) the subject provides a new set of physiological identifiers, and (ii) it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as such user; where, as defined in element (c), the stored data set includes such user's personal information and a representation of the physiological identifiers associated with such user.

Similarly, Bianco et al. also does not disclose or suggest such features. At Col. 28, line 31, through Col. 29, line 10, Bianco et al. describes a solution to the problem that individuals' biometric characteristics may change over time. For instance, if a facial image is used as a biometric identifier, the facial pattern may change, due to weight changes, aging, plastic surgery etc. Accordingly, in the passage at Col. 29, lines 5-10 that is cited in the office action, Bianco et al. describes using a second biometric device, which identifies a different biometric characteristic, when it is desired to modify a first biometric identifier. For example, if an individual's facial characteristics have changed, Bianco et al. would require a second biometric, such as a fingerprint, before allowing the facial image identifier to be modified.

Thus, Bianco et al. addresses the problem of the unreliability of biometric identifiers, in that individuals' biometric characteristics can change over time, by requiring a second biometric identifier when a first biometric has changed. However, Bianco et al. does not disclose or suggest requiring a biometric identifier at a time when a stored data set that includes a user's personal information is modified. Bianco et al. therefore does not address the problem of assuring the integrity of personal information in a stored data set. Whereas Bianco et al. concerns use of multiple biometric identifiers, an embodiment according to applicants' claim 1 relates to gating modification of personal information associated with an account.

In terms of the language of applicants' claim 1, as with Pare Jr. et al., Bianco et al. also does not disclose or suggest element (d): permitting a subject to modify information in a stored data set pertinent to a user only if (i) the subject provides a new set of physiological identifiers, and (ii) it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as such user; where, as defined in element (c), the stored data set includes such user's personal information and a representation of the physiological identifiers associated with such user.

Accordingly, because neither Pare Jr. et al. nor Bianco et al. discloses or suggests such elements of applicants' claim 1, applicants respectfully request reconsideration and allowance of claim 1.

Because independent claims 16, 17, 29, 30, and 31 include similar elements, applicants also respectfully request reconsideration and allowance of those claims, and of their dependent claims. Applicants view the term "transaction," used in claims 16, 17, 31, and 39 (claim 39 is discussed further below), broadly to include not only purchases and access to credit and cash, and other financial resources, but also access to transportation (such as airplanes and trains) and physical premises. Nevertheless, these claims are also restricted to instances wherein there is employed a database administered in such a way that modification of personal information pertaining to an individual in the data base is conditioned on a sufficient match between the stored biometric of the individual and a new biometric obtained from a person purporting to be the individual.

New Claims 36-40

Applicants respectfully request entry of new claims 36-40. New claim 36 corresponds generally to claim 1, new claims 37 and 40 correspond generally to claim 35, and new claim 39 corresponds generally to claim 16. No new matter has been introduced. It is believed that new independent claim 36 sets forth elements that distinguish from the cited references in similar ways to those discussed above. In particular, it is believed that an embodiment according to claim 36 distinguishes the cited references by requiring a comparison of a set of newly provided physiological identifiers, from a subject, with a stored set of physiological identifiers, at a time when an attempt is made to modify information in a stored data set.

New claim 37 is dependent from new claim 36, and specifies that any financial information that may be in the stored data set is not limited to that of a particular banking or financial institution.

New claim 38 is dependent from new claim 36, and specifies that obtaining the new set of physiological identifiers and permitting the subject to modify the information in the stored data set may be performed in a facility established for that purpose. Support for this claim is found in the specification at page 6, lines 10 through 22, and elsewhere.

New claim 39 is a method of authenticating a user transaction, which involves accessing information from a data base that is administered in a fashion analogous to that of the data base of claim 36.

New claim 40 is dependent from new claim 39, and specifies that any financial information that may be in the stored data set is not limited to that of a particular banking or financial institution.

Summary of Examiner Telephone Interview

Bruce D. Sunstein and Keith J. Wood (Attorneys for Applicants), and Examiner James Reagan discussed the case in a telephone interview of August 16, 2002.

Mr. Sunstein discussed how an embodiment according to the invention addresses certain possible techniques of identity theft; in a particular example of such a problem, an identity thief may change a person's bank account correspondence address to be the identity thief's address. To address this potential problem, an embodiment according to the invention requires a biometric match before permitting modification of personal information in an appropriate data base. As discussed further above, whereas Bianco et al. deals with use of multiple biometric identifiers, and Pare Jr. et al. involves access to ATM networks, a distinction over these references is found in element (d) of applicants' claim 1. This element requires a biometric match before permitting modification of personal information in an appropriate data base.

Mr. Sunstein also discussed a distinction of an embodiment according to the invention over public/private key encryption systems. Such encryption systems correspond to token-based security techniques: a private key is like a physical key in being a token, so that a thief who steals a computer with a private key on it can steal the data that the private key accesses. Such token-based security techniques differ from biometric techniques, since a computer thief does not gain possession of the owner's own physical characteristics (such as a fingerprint, voice pattern, etc.). In general, security techniques can be divided into those based on "something you know," (a secret, such as a password), "something you have," (a token), or "something you are," (a biometric characteristic). With these distinctions in mind, Mr. Sunstein submitted that applicants are aware of no case in which a biometric match is required for modification of personal information in an appropriate data base.

Conclusion

It is believed the application is now in condition for allowance. Consideration of claims 1-40 and issuance of a notice of allowance are respectfully requested.

If any additional fees are required for the timely consideration of this application, please charge deposit account number 19-4972.

Applicants believe that no extension of time is required; however, this conditional petition is being made to provide for the possibility that applicants have inadvertently overlooked the need for an extension of time.

Respectfully submitted,

Keith J. Wood
Registration No. 45,235
Attorney for Applicants

BROMBERG & SUNSTEIN LLP
125 Summer Street
Boston MA 02110-1618
Tel: 617 443 9292 Fax: 617 443 0004

211463